REMARKS

The present Amendment amends claims 2, 6, 10, 13, 17 and 21, and leaves claims 3-5, 7-9, 11, 12, 14-16, 18, 19, 22 and 23 unchanged. Therefore, the present application has pending claims 2-19 and 21-23.

Applicants' Attorney, the undersigned, wishes to thank Examiner Levitan for the courtesy extended during the interview of November 5, 2008.

During the interview it was argued that the present invention is concerned with efficiently generating a second VPN identifier on Layer 2 (L2) of the OSI Reference Model, a copy of which is attached, which is used to compose one of the plurality of Virtual Private Networks (VPNs) in a second network, based on a destination Internet Protocol (IP) address on Layer 3 (L3) and a first VPN identifier on L2, which is used to compose a first VPN in a first network, included in a packet being transmitted from the first network to the second network.

During the interview Examiner Levitan recognized that the features regarding the first and second VPN identifiers being on L2 and the destination IP address being on L3 are not taught or suggested by the references of record. During the interview, Examiner Levitan alleged that such features are not recited in the claims.

Applicants do not agree. Applicants submit that the features regarding the first and second VPN identifiers being on L2 and the destination IP address being on L3 are well known and as such need not be recited in the claims. However, in order to expedite prosecution of the present application the present Amendment amends the claims to more clearly recite that the first and second VPN identifiers are on L2 and the destination IP address is on L3.

Claims 2-19 and 21-23 stand rejected under 35 USC §103(a) as being unpatentable over McCloghrie (U.S. Patent No. 6,035,105) in view of Applicants' alleged admitted prior art (articled entitled "Use of IPsec Protocol in IP Networks"). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now recited in claims 2-19 and 21-23 are not taught or suggested by McCloghrie or Applicants' alleged admitted prior art whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims to more clearly describe features of the present invention as recited in the claims. Particularly, amendments were made to the claims to recite that the present invention is directed to a packet communication apparatus, system and method implemented in the packet communication apparatus.

According to the present invention the packet communication apparatus transmits a packet from a first network comprising a first Virtual Private Network (VPN) to a second network comprising a plurality of VPNs, wherein the packet includes a destination Internet Protocol (IP) address on Layer 3 (L3) or higher, and a first VPN identifier on Layer 2 (L2) used to compose the first VPN in the first network.

Further, according to the present invention the packet communication apparatus includes a packet generating unit which generates a second VPN identifier on L2 used to compose one of the plurality of VPNs in the second network based on the destination IP address on L3 and the first VPN identifier

on L2, and a transmitter which transmits a packet having added thereto said second VPN identifier on L2, wherein the first VPN on L2 is interconnected to the plurality of VPNs in the second network

In the present invention by using the destination IP address on L3 or higher and the first VPN identifier on L2, used to compose the first VPN in the first network, the second VPV identifier on L2, used to compose one of the plurality of second VPNs in the second network, is decided. This feature of the present invention allows for the packet communication apparatus to decide the second VPN identifier on L2 appropriately under a situation where the first VPN is interconnected to the plurality of VPNs. Without using this feature of the present invention, and under the situation where the first VPN is interconnected to the plurality of VPNs, the packet communication apparatus cannot decide the second VPN identifier and transmit the packet appropriately so as to avoid communication conflicts. More specifically by using the above described features of the present invention, packets can be transferred in the VPNs composed over the two networks so as to be prevented the packets of a particular traffic from mixing with packets belonging to other traffic, attention is directed to page 6 line 38-41 of the present application.

As discussed in the "Background of the Invention" section of the present application Applicants have recognized that if only the destination IP address is used to decide the second VPN identifier of a second network of a packet from a first network having a first VPN identifier, then it is possible for the packet communication apparatus to transmit the packet to the wrong destination because there can be an address conflict between destinations which are in different networks relative to each other. Further, if only the first

VPN identifier, used to compose the first VPN, is used to decide the second VPN identifier, then the packet communication apparatus cannot decide the second VPN identifier and transmit the packet appropriately because the packet communication apparatus cannot select one second VPN as a route of transmitting the packet among the plurality of second VPNs each of which is interconnected to the first VPN.

The present invention overcomes the above noted problems.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly, the above described features of the present invention as now more clearly recited in the claims are not taught or suggested by McCloghrie or Applicants' alleged admitted prior art whether taken individually or in combination with each other as suggested by the Examiner.

McCloghrie discloses local area network (LAN) switch interworking between virtual local area networks (VLAN's) by using a VLAN management identifier (ID) (see McCloghrie's spec. col. 4 line 62 – col. 5 line 4).

McCloghrie discloses VLAN technology which identifies the outgoing tag by using only database 205, wherein the database includes only correspondence information of VLAN management IDs (specific Layer 2 information) of different VLANs (see McCloghrie's spec. col. 4 line 62 - col. 5 line 4).

Applicants' alleged admitted prior art simply teaches the composing of VPNs in an IP environment. Thus, Applicants' alleged admitted prior art simply discloses basic IP routing technology wherein each packet includes an

IP address identifying a destination for the packet even though such destinations are entities that exist in a VPN.

In the Office Action the examiner alleges on page 7 thereof that it would have been obvious to one of ordinary skill in the art at the time the invention was made to add using IP networks and packets with IP address of Applicants' alleged Admitted Prior Art to the system of McCloghrie to implement a method allegedly widely used in IP networks.

Applicants do agree with the Examiner's allegation. Applicants submit that If one of ordinary skill in the art at the time the invention was made applied the VLAN technology of McCloghrie to the IP environment, then the resulting combination would not be the same technology as the present invention as recited in the claims.

McCloghrie fails to teach or suggest that it is directed to the problem solved by present invention as recited in the claims. Applicants submit that they have examined the problems which arise when a VPN is composed over a plurality of ISP networks, attention is directed to page 4, lines 15-18 of the present application. One of problems addressed by the present invention is that if the capsule header (first VPN identifier) given in the first network to compose the first VPN is removed in the process of retrieving the IP address of the destination, then the packets from the first VPN are mixed with packets in other networks in the interwork router, attention is directed to page 4, line 24 through page 5, line 6 of the present application. Once the interwork router removes the capsule header of a received packet, then the receiving Internet Service Provider (ISP) cannot distinguish the received packet from other packets, if the received packet has the same address as the other

packets. In the present invention this problem is solved by the interwork router generating the second VPN identifier based on not only the destination IP but also the first VPN identifier, thereby generating a unique second VPN identifier that takes into account the first VPN so as to avoid the above describe problem where the receiving Internet Service Provider (ISP) cannot distinguish the received packet from other packets.

McCloghrie merely discloses VLAN technology in interconnected L2 networks wherein the LAN switch identifies the outgoing VLAN tag of the network to which the packet is to be transmitted by using the information of the incoming VLAN tag L2 of the network from which the packet is received. Using VLAN tag which are on L2 are sufficient to transmit data on interconnected L2 networks. The problem to which the present invention is directed does not occur in the interconnected L2 networks as disclosed by McCloghrie.

McCloghrie does not even address the problem to which the present invention is directed in that the VLAN technology as taught by McCloghrie simply identifies the outgoing VLAN tag by using only database 205 and the incoming VLAN tag. The database 205 as clearly taught by McCloghrie includes only correspondence information of VLAN management IDs (specific Layer 2 information) of different VLANs, attention is directed to col. 4, line 62 through col. 5, line 4 of McCloghrie.

Thus, in McCloghrie the outgoing VLAN tag on L2 is generated based on the incoming VLAN tag on L2. Therefore, to simply add the teaching of Applicants' Alleged Admitted Prior Art to McCloghrie regarding the use of IP addresses in the IP environment would not solve the problem to which the

present invention is directed. Specifically if McCloghrie is combined with Applicants' Alleged Admitted Prior Art in the manner suggested by the Examiner in the Office Action, then the output VLAN identifier of the second VLAN is decided based only on the destination IP address not the VLAN identifier of the first VLAN and the destination IP address as in the present invention.

The above result of combining McCloghrie with Applicants' Alleged Admitted Prior Art in the manner suggested by the Examiner in the Office Action occurs due to the fact that packet communication has to follow the OSI reference model (see attached). If packet communication does not follow the OSI reference model, the packet does not communicate accurately.

Accordingly when the OSI reference model is followed, an IP router upon receipt of a packet including L2 and L3 information terminates the L2 information and retrieves routes to identify an output port based on the L3 information. Therefore, in McCloghrie the LAN switch simply changes the first VLAN tag (L2 information) to the second VLAN tag (L2 information) since no L3 information is present nor is communication on L3 intended.

However, in an ordinary IP environment, L2 information including the VLAN tag is completely dependent on the IP address, L3 information, since the network should remain in compliance with the OSI reference model. In the OSI reference model, the lower layer is completely dependent, subservient, to the higher layer. In otherwords when implementing the OSI reference model the lower layer output information to be used to transmit a packet including lower layer input information and higher layer input information is decided

based only on the higher layer input information not the higher layer input information and the lower layer input information as in the present invention.

The present invention as now recited in the claims departs from the requirements of the OSI reference model since as described above it generates the lower layer output information to be used to transmit a packet including lower layer input information and higher layer input information based on the higher layer input information and the lower layer input information, rather than only the higher layer input information as required by the OSI reference model.

As per the above the present invention implements its departure from the requirements of the OSI reference model by providing an interwork router which retrieves routes and generates the second VPN identifier (L2) based on the first VPN identifier (L2) and the destination IP address (L3). This departure from the requirements of the OSI reference model implemented by the interwork router means that the interwork router violates the border of L2 and L3. There is absolutely no teaching or suggestion of this type of violation of the border of L2 and L3 of the OSI reference model in McCloghrie or Applicants' Alleged Admitted Prior Art whether taken individually or in combination with each other as suggested by the Examiner in the Office Action.

Thus, each of McCloghrie and Applicants' alleged admitted prior art fails to teach or suggest a packet communication apparatus transmits a packet from a first network comprising a first Virtual Private Network (VPN) to a second network comprising a plurality of VPNs, wherein the packet includes a destination Internet Protocol (IP) address on Layer 3 (L3) or higher, and a

first VPN identifier on Layer 2 (L2) used to compose the first VPN in the first network as recited in the claims.

Further, each of McCloghrie and Applicants' alleged admitted prior art fails to teach or suggest a packet generating unit which generates a second VPN identifier on L2 used to compose one of the plurality of VPNs in the second network based on the destination IP address on L3 and the first VPN identifier on L2, and a transmitter which transmits a packet having added thereto said second VPN identifier on L2, wherein the first VPN on L2 is interconnected to the plurality of VPNs in the second network as recited in the claims.

Therefore, each of McCloghrie and Applicants' alleged admitted prior art fails to teach or suggest the features of the present invention as now more clearly recited in the claims and as such does not render obvious the claimed invention when combined with each other. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 2-19 and 21-23 is respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 2-19 and 21-23.

In view of the foregoing amendments and remarks, applicants submit that claims 2-19 and 21-23 are in condition for allowance. Accordingly, early allowance of claims 2-19 and 21-23 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any

overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (501.37526CX1).

Respectfully submitted,
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120

The OSI Reference Model — Understanding Layers

~ By Charlie Schluting

It is time to take a trip up the OSI Reference Model, and learn what this mysterious thing is all about. The network stack is of great significance, but not so much that it's the first thing you should learn. Many so-called networking classes will start by teaching you to memorize the name of every layer and every protocol contained within this model. Don't do that. Do realize that layers 5 and 6 can be completely ignored, though.

The International Standards Organization (ISO) developed the OSI (Open Systems Interconnection) model. It divides network communication into seven layers. Layers 1-4 are considered the lower layers, and mostly concern themselves with moving data around. Layers 5-7, the upper layers, contain application-level data. Networks operate on one basic principle: "pass it on." Each layer takes care of a very specific job, and then passes the data onto the next layer.

The physical layer, layer 1, is too often ignored in a classroom setting. It may seem simple, but there are aspects of the first layer that oftentimes demand significant attention. Layer one is simply wiring, fiber, network cards, and anything else that is used to make two network devices communicate. Even a carrier pigeon would be considered layer one gear (see RFC 1149). Network troubleshooting will often lead to a layer one issue. We can't forget the legendary story of CAT5 strung across the floor, and an office chair periodically rolling over it leading to spotty network connectivity. Sadly, this type of problem is quite common, and takes the longest to troubleshoot.

Layer two is Ethernet, among other protocols; we're keeping this simple, remember. The most important take-away from layer 2 is that you should understand what a bridge is. Switches, as they're called nowadays, are bridges. They all operate at layer 2, paying attention only to MAC addresses on Ethernet networks. If you're talking about MAC address, switches, or network cards and drivers, you're in the land of layer 2. Hubs live in layer 1 land, since they are simply electronic devices with zero layer 2 knowledge. LDon't worry about the details for now, just know that layer 2 translates data frames into bits for layer 1 processing.

You might want to go back and re-read that before moving on, because fledgling network admins always seem to mix up layers two and three.

Key Terms To Understanding Layers

ARP
Short for Address Resolution Protocol, a network layer protocol used to convert an IP address into a physical address, such as an Ethernet address.

broadcast
In networking, a distinction is made between broadcasting and multicasting. Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.

MAC
Short for Media Access Control. See MAC address or MAC layer.

subnet
A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix.

UDP
A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

If you're talking about an IP address, you're dealing with layer 3 and "packets" instead of layer 2's "frames." IP is part of layer 3, along with some routing protocols, and ARP (Address Resolution Protocol). Everything about routing is handled in layer 3. Addressing and routing is the main goal of this layer.

Layer 4, the transport layer, handles messaging. Layer 4 data units are also called packets, but when you're talking about specific protocols, like TCP, they're "segments" or "datagrams" in UDP. This layer is responsible for getting the entire message, so it must keep track of fragmentation, out-of-order packets, and other perils. Another way to think of layer 4 is that it provides end-to-end management of communication. Some protocols, like TCP, do a very good job of making sure the communication is reliable. Some don't really care if a few packets are lost--UDP is the prime example.

And arriving at layer 7, we wonder what happened to layer 5 and 6.

In short: They're useless.

A few applications and protocols live there, but for understanding networking issues talking about these provides zero benefit. Layer 7, our friend, is "everything." Dubbed the "Application Layer," layer 7 is application-specific. If your program needs a specific format for data, you invent some format that you expect the data to arrive in and you've just created a layer 7 protocol. SMTP, DNS and FTP are all layer 7 protocols.

The most important thing to learn about the OSI model is what it really represents.

Pretend you're an operating system on a network. Your network card, operating at layers 1 and 2, will notify you when there's data available. The driver handles the shedding of the layer 2 frame, which reveals a bright, shiny layer 3 packet inside (hopefully). You, as the operating system, will then call your routines for handling layer 3 data. If the data has been passed to you from below, you know that it's a packet destined for yourself, or it's a broadcast packet (unless you're also a router, but never mind that for now). If you decide to keep the packet, you will unwrap it, and reveal a layer 4 packet. If it's TCP, the TCP subsystem will be called to unwrap and pass the layer 7 data onto the application that's listening on the port it's destined for. That's all!

When it's time to respond to the other computer on the network, everything happens in reverse. The layer 7 application will ship its data onto the TCP people, who will stick additional headers onto the chunk of data. In this direction, the data gets larger with each progressive step. TCP hands a valid TCP segment onto IP, who give its packet to the Ethernet people, who will hand it off to the driver as a valid Ethernet frame. And then off it goes, across the network. Routers along the way will partially disassemble the packet to get at the layer 3 headers in order to determine where the packet should be shipped. If the destination is on the local Ethernet subnet, the OS will simply ARP for the computer instead of the router, and send it directly to the host.

Grossly simplified, sure; but if you can follow this progression and understand what's happening to every packet at each stage, you're just conquered a huge part of understanding networking. Everything gets horribly complex when you start talking about what each protocol actually does. If you are just beginning, please ignore all that stuff until you understand what the complex stuff is trying to accomplish. It makes for a much better learning endeavor!

Did You Know...

Layer two data is called a frame, and doesn't involve IP addresses. IP addresses and packets are layer 3, MAC addresses are layer 2!

Related Terminology: Webopedia > Networks > Networking Standards >

~ By Charlie Schluting
Adapted from Enterprise Networking Planet
Last updated: January 13, 2005